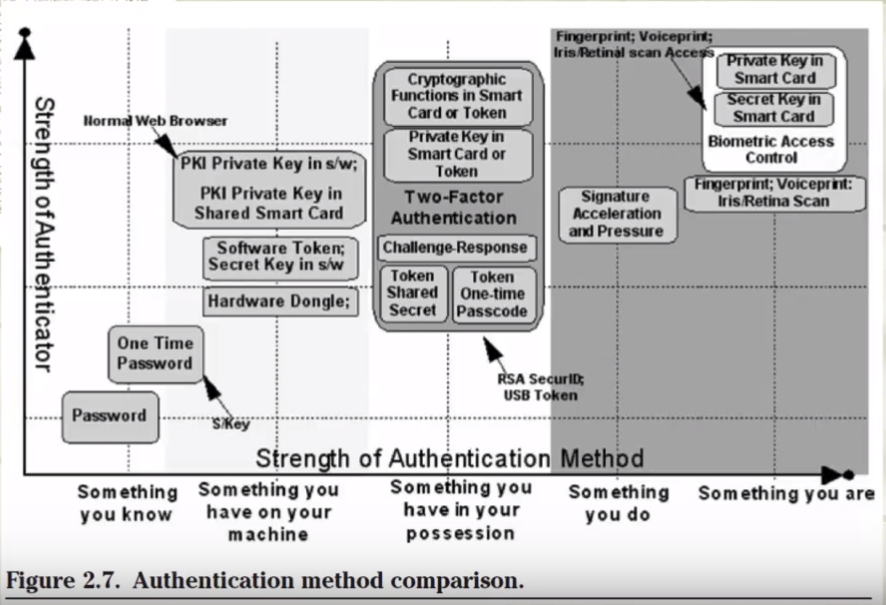
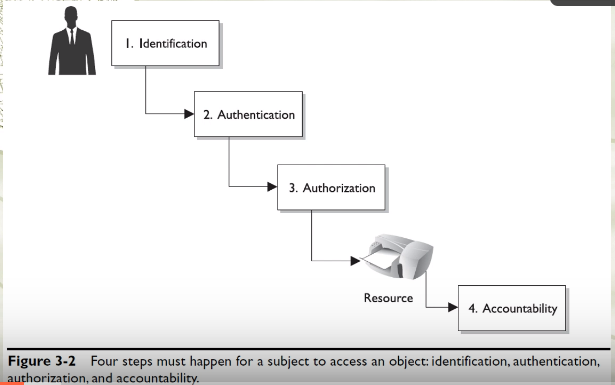
****

**Access Control Practices**

1. Deny access to systems to undefined users or anonymous accounts

Example

* Disable guest log-in function and only allow authorised users to access the systems

1. Limit and monitor usage of administrator and other powerful accounts

Example

* Use normal accounts more frequently instead, to prevent malicious softwares to exploit the power of administrator accounts

1. Suspend or delay access capability after a specific number of unsuccessful log on attempts.
2. Remove obsolete accounts as soon as the user leaves the company.

* Prevent old employees from using their account to access materials in the company after they have left the company

1. Suspend inactive accounts after 30 to 60 days.
2. Enforce strict access criteria

* Access controls - Certain files could only be accessed by certain users

1. Enforce the need-to-know and least-privilege practices (Security methods)

* Only give power when necessary

1. Disable unneeded system features, services and ports

Examples

* Uninstall unnecessary applications (esp those that may come naturally with the operating system (System hardening))

1. Replace default password settings on accounts
2. Limit and monitor global access rules
3. Remove redundant resource rules from accounts and group memberships
4. Remove redundant user IDs, accounts, and role-based accounts from resource access lists.

Examples

* When role of a user changes, the user id should be removed from the access list associated with that role

1. Enforce password rotation.
2. Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
3. Audit system and user events and actions, and review reports periodically.
4. Protect audit logs.

**Security Controls**

* Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected
* Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors
* Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network
* Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)
* Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

eg. Speeding(have fines and punishment, and preventive controls like speed bumps, detection – security cameras)

**Administrative Controls**

Risk management

Evaluate the risks and try to address them

Screening of personnel

Do background checks on people before hiring them

Security-awareness training

Change control procedures

**Technical Controls**

* also called logical controls
* implementing and maintaining access control mechanisms
* password and resource management
* identification and authentication methods
* security devices

Firewalls, Anti-virus softwares

* configuration of the infrastructure in a security aware way
* Encryption
* Authentication measures
* Smart cards
* Network authentication
* Make sure to patch software on time
* Have intrusion detection and prevention systems
* Access control lists (ACLs)
* File integrity auditing software
* Patching
* IPS
* Detective
* Security logs
* NIDS
* HIDS
* Corrective/Recovery
* IPS
* Restore from backups
* patching

**Physical Controls**